Stockholms Universitet
Institutionen för Data och Systemvetenskap
Johan Andersson

Diskret Matematik
Vårterminen 2012
2012-03-02

Inlämningsuppgifter - Restuppgifter - Omgång 2

Inlämningsuppgifterna skall lösas individuellt, samt lämnas in i samband med första tentan i Mars (+ max 3 dagar, dvs Måndagen den 19:e Mars 2012), eller andra tentan i Maj (Dvs senast den 5:e Maj 2012).

Satsa på att lämna in inlämningsuppgiften redan i Mars även om ni inte klarat alla uppgifter. Jag kommer den här gången att indikera om det skriftliga är tillräckligt för att gå vidare till en muntlig examination, och om ni inte har gjort tillräckligt kommer jag att tala om vad ni behöver förbättra (Vilka uppgifter som blev fel), så får ni en ny chans i Maj.

Ni skall vara beredda på att presentera lösningarna på uppgifterna i smågrupper.

Talteori

1. Skriv talen 55 och 101 med basen 3.
2. Skriv talen $(503)_7$ samt $(1121)_3$ på decimalform (med basen 10).
3. Beräkna $\text{SGD}(7^{100} \cdot 3^{20}, 6^5 \cdot 5^9)$.
4. Beräkna $\text{SGD}(1496, 1241)$ med hjälp av Euklides algoritm.
5. (a) Beräkna $\text{SGD}(77, 38)$ med hjälp av Euklides algoritm
   (b) Finn den allmänna lösningen till den Diofantiska ekvationen
   $$77x + 38y = 1.$$
   (c) Bestäm alla positiva heltalslösningar till ekvationen
   $$77x + 38y = 10000.$$
6. Beräkna (utan miniräknare!)
   (a) den principala resten av $33^3 \cdot 44^2 \cdot 55^4 - 10^{16}$ vid division med 13.
   (b) sistasiffran i talet $1^1 + 2^4 + 3^9 + 4^{16} + 5^{25} + 6^{36} + 7^{49} + 8^{64} + 9^{81}$.
   (c) vilken veckodag det är om 2^{32} dagar om det är Måndag idag.
   (d) vad klockan är om 5^{37} timmar om klockan är 11 på förmiddagen just nu.
7. Bevisa att om n är ett udda tal så är $n^2 - 1$ delbart med 8.
8. Bevisa att $\sqrt{3} - 2\sqrt{5}$ är ett irrationellt tal.
9. Första steget i att bestämma en nyckel i RSA-algoritmen är att bestämma två stora primtal p och q. För tal av den storleksordningen som behövs för RSA finns det nu visserligen tillräckligt snabba algoritmer för att bevisa att tal är primtal (och i praktiken räcker det med att visa att talen "nästan säkert" är primtal (är sk pseudoprimtal)). Dock är det så att det finns ännu snabbare sätt att bevisa att tal på en viss form är primtal. Till exempel finns det mycket effektiva sätt att avgöra om tal på formen
   $$2^n - 1$$
   är primtal. När dessa tal är primtal så kallas de för Mersenneprimtal.

(a) Förklara varför är det inte en bra ide att använda Mersenneprimtal i RSA-algoritmen.

(b) En nyligen upptäckt svaghet i vissa nycklar för RSA (Februari 2012) bygger på samma princip som i (a) uppgiften. Leta reda på svagheten (genom att exempelvis googla "RSA 99.8") och förklara den.

10. Utför multiplikationen av 13 och 25

    (a) på vanligt sätt.

    (b) med Karatsubamultiplikation.

Relationer

1. Avgör om relationen $R = \{(1,1),(2,1),(3,3),(3,2)\}$ på mängden $A = \{1,2,3\}$ är reflexiv, antisymmetrisk, respektive transitiv.

2. Avgör vilka av följander relationer på $\mathbb{Z}^+$ som är reflexiva, symmetriska, respektive transitiva, samt vilka som är ekvivalensrelationer.

    (a) aRb omm $(ab)|36$.

    (b) aRb omm ab är kvadraten av ett heltal.

3. Låt $\{1,2\},\{3\},\{4\},\{5,6\}$ vara en partition av mängden $A = \{1,2,3,4,5,6\}$ och låt R vara den ekvivalensrelation som ger upphov till partitionen. Ange ekvivalensrelationen $R \subseteq A \times A$ som en mängd av talpar.

4. Låt S vara en relation på en mängd A. Definiera relationen R på $A \times A$ genom

    (a) $(a,b)R(c,d)$ om och endast om aSc.

    (b) $(a,b)R(c,d)$ om och endast om aSc eller bSd.

    (c) $(a,b)R(c,d)$ om och endast om aSc och bSd.

    Avgör följande.

    (a) Om S är en ekvivalensrelation, vilka av ovanstående relationer måste vara symmetriska, reflexiva och/eller transitiva. Vilka är ekvivalensrelationer?

    (b) Om S är en partiell ordning, vilka av ovanstående relationer måste vara antisymmetriska, reflexiva och/eller transitiva. Vilka är partiella ordningar?

    (c) Om S är en funktions graf, dvs $S = \{(x, f(x)) : x \in A\}$, vilka av ovanstående relationer är en annan funktions graf, dvs $R = \{(x, g(x)) : x \in A \times A\}$?